UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,315	03/24/2004	David M. Durham	42P19299	6493

8791 7590 12/21/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
SCHMIDT, KARI L	
ART UNIT	**PAPER NUMBER**
2139	
MAIL DATE	**DELIVERY MODE**
12/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	**Application No.** 10/809,315	**Applicant(s)** DURHAM ET AL.	
	Examiner Kari L. Schmidt	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 15 October 2007.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-38 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-38 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 10/15/2007,11/9/2007.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response to the amendment filed on 10/15/2007. Claims 1-38 are pending. Claims 11, 19, 22, 25, 29 and 31 have been amended. The examiner maintains the same grounds of rejection as in previous office action mailed out on 7/13/2007. The examiner has responded to the arguments presented by the Applicants. This action is made final.

Claim Objections

The claim objection regarding Claim 31 is withdrawn.

Claim Rejections - 35 USC § 112

The 35 U.S.C. 112, second paragraph rejections regarding Claims 6, 19, 22, and 25 have been withdrawn.

Claim Rejections - 35 USC § 101

The 35 U.S.C. 101 regarding Claims 29-38 have been withdrawn.

Response to Arguments

Applicant's arguments filed 10/15/2007 have been fully considered but they are not persuasive.

The applicant argues that Baldwin fails to teach "not directly accessible to a host processor on the client" as found in claims 1, 11, 22, and 29. The examiner disagrees.

The examiner notes that Baldwin teaches "not directly accessible to a host processor on the client" (see at least, [0067]). The examiner notes that a cryptographic engine (CryptoEngine) performs in a restricted mode that is only accessible during normal operation by transferring control from a normal mode of the processor to a restricted mode of the processor via CryptoGate. The examiner notes a “restricted mode" is not directly accessible to a host processor on a client. The examiner notes that a “restricted mode" is a secure mode govemed by the CryptoEngine in which the CryptoEngine controls sensitive data (e.g. symmetric-key) exchange. The examiner notes that the processor during "normal mode" is not privy to sensitive data (e.g. symmetric-key) exchange (see at least, [0224]: the examiner notes the ROM component runs in SMM, which is a restricted mode of a processor). The examiner notes the CryptoEngine uses nonvolatile memory and privileged processing mode to perform cryptographic features (see at least, [0073]). The examiner notes that the host processor of client does not have access to the embedded agent data and symmetric cryptographic keys only the CryptoEngine running in a restricted mode. Further the examiner notes that "a storage" is the non-volatile memory (see at least, [0224]), the “a network link” is the SSL/TLS secured connections (see at least, [0085], and the “communication channel” is the SSL/TLS secured connections (see at least, [0085]). The examiner notes these argument are not persuasive and therefore the rejection is maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-38 are rejected under 35 U.S.C. 102(b) as being anticipated by Baldwin et al. (US 2004/0039924 A1).

Claim 1, 11, 22, and 29

Baldwin discloses a method comprising: provisioning a symmetric cryptographic key across multiple clients through multiple embedded agents (see at least, [0208]: " the clients (multiple clients) identify themselves using..."), each client having one of the embedded agents, one embedded agent in each client having an embedded agent to store the symmetric cryptographic key in a storage accessible to the embedded agent and not directly accessible to a host processor on the client (see at least, Figure 1, [0067]: " the cryptographic engine performs cryptographic operations in a restricted mode that is only accessible during normal operation by transferring control from a normal mode of the processor to a restricted mode of the processor via CryptoGate... symmetric key(s) and of performing symmetric cryptographic and public key cryptography and of pseudo random number generation, an optionally of private key cryptography..."); and providing access to an encrypted traffic flow in a network to a client if the client is authenticated with the key (see at least Figure 4, [0695-0700]:

"multi-factor client authentication application for accessing a virtual private network... software component running on a Device Authority server connected to the internet and with access to a database of KID/DMK pairs...")

Claim 2, 12, 13, and 23

Baldwin discloses a method according to claim 1, wherein provisioning the key through the embedded agents further comprises provisioning the key through an embedded agent having network access via a network link not visible to a host operating system (OS) running on the client (see at least, Figure, Figure 4, [0694-0700]: "VPN"; [0067]: " the cryptographic engine performs cryptographic operations in a restricted mode that is only accessible during normal operation by transferring control from a normal mode of the processor to a restricted mode of the processor via CryptoGate... symmetric key(s) and of performing symmetric cryptographic and public key cryptography and of pseudo random number generation, an optionally of private key cryptography...")).

Claim 3, 24, 25, 30, and 31

Baldwin discloses a method according to claim 2, wherein providing access to the traffic flow if the client is authenticated comprises the embedded agent authenticating the client over the network line not visible to the host OS (see at least, Figure 1, Figure 4, [0694-0700]:"VPN: client over the network not visible to the host OS"; [0039]: "...if the unsealed AppContainer has acceptable values then the specific application on a specific device is considered to be authenticated... [0199] :"PubKContainer is a digital envelope that is sealed by the client with an RSA public key...")).

Claim 4, 14, and 32

Baldwin discloses a method according to claim 1, wherein providing access to the traffic flow further comprises providing multiple clients access with the key to nodes in the network, the nodes in the network to decrypt the traffic flow and subsequently encrypt the traffic flow to transmit the traffic to a next node in the network (see at least, Figure 4, [0704-0716]: "The VPN typically includes a number of machines that cooperate between them to grant access and block untrusted traffic..." "Process name Description MFCA Subscription Process that generates licensing information for a SAM... The ultimate purpose of this registration is to provide SAM with the appropriate App Key to seal and unseal App Containers that will be exchange with the client device... the VPN client, SAM server, and the ARM server have to be configured to be able to hand out the appropriate App Keys successfully..").

Claim 5, 18, and 33

Baldwin discloses a method according to claim 1, further comprising updating at a client the symmetric cryptographic key provisioned across the multiple clients through a public and private key exchange with a public and private key associated the client (see at least, [0075] : "perform these functions, the authentication server seals and unseals containers that are exchanged with a cryptographically-enable- d client device, using the assistance of one or more Device Authority servers as needed. The authentication server maintains a table of Key ID (KID) values... "[0176]: " an acknowledgment servlet waits for a client response and then updates the database table for permanent DMK..., [0747]: " PubK Containter using the private bit of the communication key and updates its internal tables with the new device ADID.. if everything is all right, the application registration module has the Key ID of the client device, so it finds the DMK, and computes the App Key for the given ACD...").

Claim 6, 15, 16, 17, 19, 26, and 34

Baldwin discloses a method according to claim 1, wherein providing access if the client is authenticated further comprises: the embedded agent verifying that a platform associated with the client is not compromised; and the embedded agent providing the key and an assertion that the client is not compromised to a verification entity on the network (see at least, [0015] The present invention provides a small security kernel, that facilitates the process of analyzing and establishing trust in the implementation of the kernel, while at the same time removing the limitations of the aforementioned add-on hardware solutions. Ideally, the security kernel operates in a separate domain from both the application programs (applications) and the operating system (OS) running on the host machine, and yet with access to the memory of the OS and applications. The present invention provides such a security architecture by creating a small inner security kernel within the boundaries of a traditional existing operating system, and that can verify the integrity of and perform secure operations on behalf of the OS and applications. [0016] Another important aspect of this invention is that it enables the security kernel to be tied into an infrastructure that can establish trust via between two devices (e.g., client device and DSS), in some embodiments via a shared symmetric key. [0017] Key aspects of the present invention comprise [0018] (1) Open-at-reset lockable (OAR-locked) non-volatile memory (NVM) that contains a secret master key, called the Device Master Key or DMK, which is unique to the device. The DMK is moved into SMRAM, a specially controlled region of memory that is only accessible in a System Management Mode (SMM) at startup, and whereafter OAR-locked non-volatile memory is disabled, [0019] (2) containers to bind the DMK to specific applications, and that solves privacy/user controllability problems, and [0020] (3) spot checking of the integrity of a calling application "on-the-fly". [0021] The invention also provides Application Keys that are bound to the device and to Applications, and, optionally, to Customer-Secrets provided by the Applications. A given application can have several different keys corresponding to different values of the Customer-Secret. [0230] The CustomerSecret part allows a company to discard compromised application Containers without having to get a new build for the application that would produce a different Application Code Digest. Also, this CustomerSecret allows a given instance of an application (e.g. secure logon application) on a device to securely share data with more that one server. Each server would setup a unique CustomerSecret with that same application on the same device. Thus, the sealed AppContainers could only be decrypted if the correct CustomerSecret is provided.")

Claim 7 and 35

Baldwin discloses a method according to claim 6, further comprising the embedded agent indicating to a remote network device if the client is compromised (see at least, Figure 4, [0652] Presented below is a description of the application registration module (ARM) component in the MFCA VPN product. The application registration module assists a Strong Authentication Module (SAM) in providing access to the secure App Containers that are exchanged between the client devices and cryptographically-enabled servers.").

Claim 8 and 36

Baldwin discloses a method according to claim 6, further comprising the embedded agent foreclosing network access to the client if the client is compromised (see at least, Figure 1, Figure 4, [0029]: "Another exemplary system for hiding a master cryptographic key in storage comprises power-on software that reads a master key from non-volatile storage, closes access to the non-volatile storage such that access does not become available again until the next system reset, and writes sensitive data derived from the master key to a hidden address space, and wherein only a program that runs in a restricted operational mode of the system has access to the sensitive data in the hidden address space." [0090] The protected non-volatile memory 11 is used to store the secret device master key. The BIOS system initialization module 12 is responsible for securely transferring the secret DMK from non-volatile memory 11 into SMRAM 13, a protected memory region that is only addressable from SMM 16. After the DMK is transferred into SMRAM 13, the system initialization module 12 closes the OAR-lock latch 14 to render the non-volatile memory 11 inaccessible to programs 15 running in the system until the next system reset. The DMK is only available in hidden SMRAM 16 during normal operation of the system. ").

Claim 9, 20, 27 and 37

Baldwin discloses a method according to claim 1, further comprising the embedded agent performing cryptographic functions on data with the key to authenticate data with the key (see at least, [0067] The cryptographic engine (CryptoEngine) performs cryptographic operations in a restricted mode that is only accessible during normal operation by transferring control from a normal mode of the processor to a restricted mode of the processor via CryptoGate. The restricted mode operations may also include operations where sensitive data is available to the processor during secure bootstrap and Power-On Self-Test operations. The CryptoEngine is capable of storing and recalling high integrity public keys, and of storing at least one long-lived symmetric key (the DMK), and of deriving symmetric keys from the long-lived symmetric key(s), and of performing symmetric cryptography (both integrity and privacy primitives) and public key cryptography, and of pseudo random number generation, and optionally of private key cryptography, and optionally of other cryptographic support functions such a key generation and importing and exporting keys. Some embodiments of the CryptoEngine may use specialized cryptographic hardware, such as smartcards, or a

TCPA TPM." Abstract: System and method for securing a computing device using a master cryptographic key that is bound to the device. The master key is used to derive sensitive data that is transferred to storage that is only accessible in a restricted mode of operation. The master key is used to derive one or more application keys that are used to secure data that is specific to an application/device pair. Non-privileged programs can request functions that run in a more restricted mode to use these application keys. The restricted mode program checks the integrity of the non-privileged calling program to insure that it has the authority and/or integrity to perform each requested operation. One or more device authority servers may be used to issue and manage both master and application keys.).

Claim 10, 21, 28 and 38

Baldwin discloses a method according to claim 1, further comprising the embedded agent including a derivative of the key in a header of data to be transmitted to authenticate the data with the key (see at least, [0198], [0247], [0279]: "AppContainer is a protected container that can only be read or written by a specific application program running on a specification machine... bound to a given machine by using a derivative of the DMK for encryption..." Abstract: The master key is used to derive sensitive data that is transferred to storage that is only accessible in a restricted mode of operation. The master key is used to derive one or more application keys that are used to secure data that is specific to an application/device pair. Non-privileged programs can request functions that run in a more restricted mode to use these application keys. The restricted mode program checks the integrity of the non-privileged calling program to insure that it has the authority and/or integrity to perform each requested operation. One or more device authority servers may be used to issue and manage both master and application keys.").

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100